ELSEVIER

Discrete Mathematics 138 (1995) 161–167

DISCRETE MATHEMATICS

Mendelsohn designs associated with a class of idempotent quasigroups☆

Darryn E. Bryant, Sheila Oates-Williams*

Centre for Combinatorics, Department of Mathematics, The University of Queensland, Brisbane, Queensland 4072, Australia

Received 7 July 1993; revised 14 December 1993

Abstract

The groupoid operation defined by $x * y = -\mu x + (1+\mu)y$ on finite fields was used by Mendelsohn to construct cyclic designs. We investigate the more general situation where the underlying structure is $\mathbb{Z}_n$, with n odd, but not necessarily prime.

1. Introduction

In his paper [6], Mendelsohn introduced the concept of *perfect cyclic designs*, now generally known as *Mendelsohn designs*. A Mendelsohn design can be thought of as a decomposition of a λ-fold complete, directed, loopless graph into a collection of directed cycles of length k such that the edge set of the graph is partitioned. If every ordered pair of distinct vertices occurs in the cycles precisely λ times at a distance t apart, the design is said to be *t-perfect*, see [3, 4]. A design is *perfect* if it is t-perfect for $t = 1, 2, \ldots, k-1$. Mendelsohn gave a technique for constructing such designs, with $\lambda = 1$, using quasigroups derived from Galois fields. He defined an operation $*$ on GF(q) by $x * y = -\mu x + (1+\mu)y$, where μ is a primitive kth root of unity and showed that the cycles of the form $(a, b, a*b, b*(a*b), (a*b)(b*(a*b)), \ldots)$ (where the vertices of the graph are labelled with the elements of the field) yield a perfect k-cycle system of order q with $\lambda = 1$. The case $\mu = -\frac{1}{2}$ is of particular interest, because the quasigroup then obtained is commutative, and, when q is prime, it is the idempotent commutative quasigroup which plays such an important role in the construction of Steiner triple systems. The above quasigroup can be defined on $\mathbb{Z}_n$ for any odd n, not merely for n an odd prime, and, in general, the operation $*$ will define a quasigroup on $\mathbb{Z}_n$ provided

☆This work was supported by a grant from the Australian Research Council.
*Corresponding author. E-mail: sw@maths.uq.oz.au.

SSDI 0012-365X(94)00197-9

both $-\mu$ and $1+\mu$ are units in $\mathbb{Z}_n$ (so n is odd). In this paper we investigate the designs that are obtained in this more general situation, determining cycle lengths and proving resolvability.

Lindner and Mendelsohn [5] consider another interesting case, again over a finite field, namely $\mu=1$. In this situation $*$ becomes $x*y=-x+2y$, and we have cycles of length p. Since $(x*y)*y=x$, each cycle occurs with its reverse, so we can consider the system as consisting of undirected cycles.

2. Definitions, notation and preliminary results

As usual, $\mathbb{Z}_n$ will denote the ring of integers modulo n; for our purposes n will always be odd. Then $*$ denotes the binary operation on $\mathbb{Z}_n$ defined by $x*y=-\mu x+(1+\mu)y$. We will consider only the situation where both $-\mu$ and $1+\mu$ are invertible in $\mathbb{Z}_n$, so that $(\mathbb{Z}_n, *)$ is a quasigroup. Since n is odd, $-\mu=\frac{1}{2}$ will always satisfy this condition. In [6] Mendelsohn defined cycles by $(x_0, x_1, \ldots, x_i, \ldots)$, where $x_{i+2}=x_i*x_{i+1}$. He showed that $x_i=-(\mu+\mu^2+\cdots+\mu^{i-1})x_0+(1+\mu+\mu^2+\cdots+\mu^{i-1})x_1$. Thus $x_k=x_0$ provided $(1+\mu+\mu^2+\cdots+\mu^{k-1})(x_1-x_0)=0$, and then $x_{k+1}=\mu(1+\mu+\mu^2+\cdots+\mu^{k-1})(x_1-x_0)+x_1=x_1$ so that we have cycles of length k. In the cases considered by Mendelsohn the underlying ring is a field, and so all the non-trivial cycles are of length k provided that μ is a kth root of unity.

The perfectness of these Mendelsohn systems follows from the fact that, provided $i<k$, the equation

$$-(\mu+\mu^2+\cdots+\mu^{i-1})x_0+(1+\mu+\mu^2+\cdots+\mu^{i-1})x_1=x_i$$

has a unique solution for x_1, given x_0 and x_i. The case where $n=3^\alpha$ is also of especial interest, because, if μ and $1+\mu$ are prime to 3 then, necessarily, $\mu\equiv 1 \bmod 3$.

In [2] another method of generating the cycle systems is given, using the operator $\circ$ defined by $x\circ y=\mu x+(1-\mu)y$. For μ and $1-\mu$ invertible, this is again a semigroup operation, and it is easy to check that, if y is chosen so that $x_0\circ y=x_1$, then $(x_0, x_0\circ y, (x_0\circ y)\circ y, \ldots)$ is the same cycle as the one constructed above using $*$. This formulation makes the resolvability of the designs much easier to see. We shall make particular use of the cycles obtained by taking $y=0$. These are of the form $(x, \mu x, \mu^2 x, \ldots)$ and all the other cycles can be obtained from these by cyclic generation.

Notation. We will use the notation $C(n, \mu)$ for the cycle system obtained from the ring $\mathbb{Z}_n$ (n odd), using the element μ and the operation $*$, (or $\circ$ when $1-\mu$ is also invertible).

3. General results

The first lemma of this section has the consequence that the cycle systems are always cyclically generated from an appropriate number of initial cycles.

Lemma 3.1. *If* $(x_0, x_1, \ldots, x_{k-1}) \in C(n, \mu)$ *then* $(x_0+d, x_1+d, \ldots, x_{k-1}+d) \in C(n, \mu)$ *for any integer* d.

Proof. This follows immediately from the fact that $(a+d)*(b+d) = -\mu(a+d)+(1+\mu)(b+d) = -\mu a+(1+\mu)b+d = a*b+d$. □

Since the quasigroups we are using are all idempotent, it is sometimes convenient to consider our cycle systems as containing all possible cycles of length one (i.e., loops at the vertices). We use this convention in the following theorem.

Theorem 3.2. *Let* $n=rs$ *where* $1<r$, $1<s$ *and* r *and* s *are relatively prime. Let* $\mu \in \mathbb{Z}_n$ *be such that it and* $\mu+1$ *are invertible. Let* ν *and* η *be the images of* μ *in* $\mathbb{Z}_r$ *and* $\mathbb{Z}_s$ *respectively. Let the cycle lengths of* $C(r, \nu)$ *and* $C(s, \eta)$ *be* $l_0\ (=1), l_1, \ldots, l_t$ *and* $m_0\ (=1), \ldots, m_u$, *respectively, then the cycle lengths of* $C(n, \mu)$ *are the* $\operatorname{lcm}(l_i, m_j)$s, $0 \leqslant i \leqslant t$, $0 \leqslant j \leqslant u$.

Proof. We use the isomorphism, ϕ, between $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ defined by $a\phi = (a_1, a_2)$ where $a_1 \equiv a \bmod r$ and $a_2 \equiv a \bmod s$. (The Chinese remainder theorem shows that ϕ is one-one and onto; the structure preserving properties are an obvious consequence of the properties of modular arithmetic.) Since $\mu\phi = (\nu, \eta)$, we have $a *_\mu b = (a_1 *_\nu b_1, a_2 *_\eta b_2)$ and the result on cycle lengths follows immediately. □

We now need to examine cycle systems of the form $C(p^\alpha, \mu)$. There are two cases to be considered, depending on whether or not $\mu \equiv 1 \bmod p$.

Theorem 3.3. *If* $n=p^\alpha$, *where* $\alpha \geqslant 2$ *and* $\mu \equiv 1 \bmod p$ *then* $C(n, \mu)$ *has* $p^\alpha - p^{\alpha-1}$ *cycles of length* p^β, $1 \leqslant \beta \leqslant \alpha$. *Let* p^γ *be the largest power of* p *dividing* $\mu-1$. *Then the cycles of length* p^β *can be cyclically generated from* $p^{\gamma-1}(p-1)$ *initial cycles for* $\beta > \gamma$ *and* $p^{\beta-1}(p-1)$ *initial cycles for* $\beta \leqslant \gamma$.

Proof. We first note that since $\mu \equiv 1 \bmod p$, $1+\mu+\mu^2+\cdots+\mu^{k-1} \equiv 0 \bmod p^\eta$ if and only if $p^\eta | k$. Thus the smallest value of k for which $(1+\mu+\mu^2+\cdots+\mu^{k-1})(x_1-x_0) \equiv 0 \bmod p^\alpha$ is $p^{\alpha-\delta}$ where p^δ is the highest power of p dividing x_0-x_1. Thus we obtain cycles of length p^β, $1 \leqslant \beta \leqslant \alpha$.

From the way in which the cycle $(x_0, x_1, \ldots, x_i, \ldots)$ is generated, it can be seen that $x_{i+1}-x_i = \mu^i(x_1-x_0)$. If we consider the cycle starting $(0, ap^\delta, \ldots)$, where $p \nmid a$, we have that $x_{p^\xi+1} - x_{p^\xi} = \mu^{p^\xi} ap^\delta$. Since $\mu = 1+bp^\gamma$ this is congruent to ap^δ modulo p^α when $\gamma+\delta+\xi = \alpha$. Thus a cycle of length $\beta\ (=\alpha-\delta)$ involves only $p^{\beta-\gamma}$ distinct differences for $\beta \geqslant \gamma$, and one difference for $\beta \leqslant \gamma$. Hence, to use all $p^\beta - p^{\beta-1}$ differences which are divisible by precisely p^δ we need $p^{\gamma-1}(p-1)$ initial cycles of length p^β for $\beta > \gamma$. For $\beta \leqslant \gamma$ we need $p^{\beta-1}(p-1)$ initial cycles. Since each difference is used p^α times, and each cycle of length p^β uses p^β, we have that the total number of cycles of length β is $p^{\alpha-1}(p-1)$. This means, of course, that when we generate the cycles cyclically, we get repetitions after $p^{\alpha-1}(p-1)/b$ steps, where b is the number of initial cycles. In fact,

it is easily checked that the $(p^{\beta-\gamma})$th term in the cycle beginning $(0, ap^{\delta}, \ldots)$ is $ap^{\alpha-\gamma}$ when $\beta \geqslant \gamma$. □

Theorem 3.4. *Let $n=p^{\alpha}$, where $\alpha \geqslant 2$ and let μ have order $k>1 \bmod p$ (so $1-\mu$ is invertible). If p^{γ} is the highest power of p dividing $\mu^{k}-1$ and $p-1=dk$, then $C(n,\mu)$ has $p^{\alpha}dp^{\gamma-1}$ cycles of length kp^{β}, $1 \leqslant \beta \leqslant \alpha-\gamma$ and $p^{\alpha}(p^{\gamma}-1)/k$ cycles of length k. The cycles of length kp^{β}, $1 \leqslant \beta \leqslant \alpha-\gamma$, can be cyclically generated from $dp^{\gamma-1}$ initial cycles and the cycles of length k from $(p^{\gamma}-1)/k$ initial cycles.*

Proof. We use the $\circ$ formula for the cycles in the case $y=0$. For $x \in \mathbb{Z}_{p^{\alpha}}$, let $x=ap^{\delta}$ where $p \nmid a$. Then the term x_i of the cycle beginning with $(x, \ldots)$ is given by $x_i=\mu^{i}x$, and, as above, this is congruent to x modulo p^{α} when $i=kp^{\xi}$ where $\xi+\gamma+\delta=\alpha$. Thus the length of the cycle is $kp^{\alpha-\gamma-\delta}$ for $\alpha \geqslant \gamma+\delta$ and k otherwise. Hence we have cycles of lengths kp^{β} for $0 \leqslant \beta \leqslant \alpha-\gamma$. Since there will be no repetitions of differences in the cycle, using the same argument as in the previous theorem, we see there must be $p^{\alpha-\delta-1}(p-1)/kp^{\alpha-\delta-\gamma}=dp^{\gamma-1}$ cycles of length $kp^{\alpha-\delta-\gamma}$ in the case $y=0$, for $\alpha-\delta>\gamma$, and the remaining $p^{\gamma}-1$ elements yield $(p^{\gamma}-1)/k$ cycles of length k. By cyclic generation we get cycles of the same lengths corresponding to each of the p^{α} possible values of y. □

Using Theorems 3.2–3.4 and a simple induction argument on the number of distinct primes dividing n we can determine the structure of the cycle system $C(n,\mu)$ for any odd positive integer n and any μ such that μ and $\mu+1$ are invertible. In general, our cycle systems are not t-perfect for all feasible t, since the equation

$$-(\mu+\mu^{2}+\cdots+\mu^{i-1})x_0+(1+\mu+\mu^{2}+\cdots+\mu^{i-1})x_1=x_i$$

will not be soluble for x_1 if $1+\mu+\mu^{2}+\cdots+\mu^{i-1}$ is not invertible. However, since we are using quasigroups, the systems are always 2-perfect.

4. Resolvability

Provided one is willing to allow cycles of length 1, the $C(n,\mu)$ are all resolvable. The following theorem describes the resolution classes.

Theorem 4.1.

(1) *Let $\mu \equiv 1 \bmod p$ and let p^{γ} be the highest power of p dividing $\mu-1$; then each resolution class of $C(p^{\alpha},\mu)$ contains $p^{\alpha-\beta}$ cycles of length p^{β}, $0 \leqslant \beta \leqslant \alpha$. [Note we are including the resolution class consisting of p^{α} cycles of length 1.] There are $p^{\gamma-1}(p-1)$ resolution classes containing cycles of length p^{β} for $\beta>\gamma$ and $p^{\beta-1}(p-1)$ classes for $\beta \leqslant \gamma$.*

(2) *Let μ have order k mod p ($k \neq 1$), let p^γ be the highest power of p dividing $\mu^k - 1$ and let $p - 1 = dk$; then each resolution class of $C(p^\alpha, \mu)$ contains $dp^{\gamma-1}$ cycles of length kp^β for $1 \leqslant \beta \leqslant \alpha - \gamma$, $(p^\gamma - 1)/k$ cycles of length k and one cycle of length 1.*

(3) *Let $n = rs$, where $\gcd(r, s) = 1$. Then the resolution classes of $C(n, \mu)$ may be obtained from those of $C(r, \nu)$ and $C(s, \eta)$ as follows: Let R be a resolution class of $C(r, \nu)$ containing a_i cycles of length l_i and S a resolution class of $C(s, \eta)$ containing b_i cycles of length m_i; then $C(n, \mu)$ has a resolution class containing $a_i b_j \gcd(l_i, m_j)$ cycles of length $\operatorname{lcm}(l_i, m_j)$.*

Proof. (1) and (2) follow immediately from the descriptions of the cycle systems given in Theorems 3.3 and 3.4. (3). Let $(x_1, \ldots, x_1) \in R$ and $(y_1, \ldots, y_m) \in S$ and let $d = \gcd(l, m)$ and $k = \operatorname{lcm}(l, m)$. Consider the cycles of $C(n, \mu)$ of the form

$$((x_1, y_{1+h}), (x_2, y_{2+h}), \ldots, (x_k, y_{k+h}), (x_1, y - k + 1 + h) \ldots)$$

for $0 \leqslant h < l$. Each x_i will appear m/d times in any given cycle, so to get all pairs of the form (x_i, y_j) we need d such cycles. The result now follows. □

We illustrate this result with some examples.

Examples 4.2. (1) $C(9, 4)$: a resolution class consisting of one cycle of length 9,

$$\{(0, 1, 5, 3, 4, 8, 6, 7, 2)\};$$

a resolution class consisting of three cycles of length 3,

$$\{(0, 3, 6), (1, 4, 7), (2, 5, 8)\}.$$

(2) $C(81, 10)$: a resolution class consisting of nine cycles of length 9,

$\{(0, 9, 18, 27, 36, 45, 54, 63, 72),$

$(1, 10, 19, 28, 37, 46, 55, 64, 73),$

$(2, 11, 20, 29, 38, 47, 56, 65, 74),$

$(3, 12, 21, 30, 39, 48, 57, 66, 75),$

$(4, 13, 22, 31, 40, 49, 58, 67, 76),$

$(5, 14, 23, 32, 41, 50, 59, 68, 77),$

$(6, 15, 24, 33, 42, 51, 60, 69, 78),$

$(7, 16, 25, 34, 43, 52, 61, 70, 79),$

$(8, 17, 26, 35, 44, 53, 62, 71, 80)\}.$

(3) $C(25,2)$: a resolution class consisting of one cycle of length 20, one of length 4 and one of length 1,

$$\{(1,2,4,8,16,7,14,3,6,12,24,23,21,17,9,18,11,22,19,13),(5,10,20,15),(0)\}.$$

(4) $C(25,7)$: a resolution class consisting of six cycles of length 4 and one of length 1,

$$\{(1,7,24,18),(2,14,23,11),(3,21,22,4),(6,17,19,8),(9,13,16,12),$$
$$(5,10,20,15),(0)\}.$$

(Example (4) also occurs in [1].)

(5) $C(25,6)$: a resolution class consisting of one cycle of length 25,

$$\{(0,1,7,18,9,5,6,12,23,14,10,11,17,3,19,15,16,22,8,24,20,21,2,13,4)\};$$

a resolution class consisting of five cycles of length 5:

$$\{(0,5,10,15,20),(1,6,11,16,21),(2,7,12,17,22),(3,8,13,18,23),(4,9,14,19,24)\}.$$

Notice that some of the above resolution classes correspond to multiples of consecutive powers of integers. For example, in $C(25,2)$ we have

$$\{(1,2,2^2,2^3,\ldots,2^{19}),(5,5\cdot 2,5\cdot 2^2,5\cdot 2^3),(0)\}$$

and in $C(25,7)$ we have

$$\{(1,7,7^2,7^3),(2,2\cdot 7,\ 2\cdot 7^2,2\cdot 7^3),\ldots\}.$$

5. The case $n=p(2^p-1)$.

Most of our cycle systems have cycles of varying lengths, but one case in which all the nontrivial cycles have the same length is for $n=p(2^p-1)$ (p an odd prime) and $\mu=2^{p-1}$. We have the following result.

Theorem 5.1. *Let $n=p(2^p-1)$, where p is an odd prime, and let $\mu=2^{p-1}$. Then the operation*

$$x*y=-\mu x+(1+\mu)y$$

is a quasigroup operation and the corresponding Mendelsohn system is a perfect resolvable p-cycle system.

Proof. We first note that μ and $\mu+1$ are each invertible in $\mathbb{Z}_n$. This is obvious for μ, and, since $2^{p-1}\equiv 1 \bmod p$ it is clear that $p\nmid \mu+1$. Also $2^p-1-2(2^{p-1}+1)=-3$, so the greatest common divisor of 2^p-1 and $\mu+1$ divides 3. Since p is odd, $2^{p-1}\equiv 1 \bmod 3$,

so $3 \nmid \mu+1$. Hence 2^p-1 and $2^{p-1}+1$ are relatively prime, and the result follows. Hence $*$ is a quasigroup operation. Note that, since $2^p-1-2(2^{p-1}-1)=1, \mu-1$ is also relatively prime to 2^p-1.

From the results of Mendelsohn quoted in Section 2, we know that a cycle starting $(a, b, \ldots)$ has order r, where r is the least positive integer for which

$$(1+\mu+\mu^2+\cdots+\mu^{r-1})(a-b) \equiv 0 \bmod p(2^p-1).$$

Since $\mu \equiv 1 \bmod p$, and μ has order p modulo 2^p-1, we have that $1+\mu+\mu^2+\cdots+\mu^{r-1} \equiv 0 \bmod p$, 2^p-1 or $p(2^p-1)$ if and only if $p \mid r$. If $p \nmid r$ then the above equation is satisfied if and only if $(a-b) \equiv 0 \bmod p(2^p-1)$. Hence all cycles have length p.

Resolvability follows from Theorem 4.1 and perfectness from the fact that the equation

$$-(\mu+\mu^2+\cdots+\mu^{i-1})x_0+(1+\mu+\mu^2+\cdots+\mu^{i-1})x_1=x_i$$

will be uniquely soluble for x_1 for all $i<p$. □

References

[1] I. Anderson and N.J. Finizio, Cyclic whist tournaments, Discrete Math. 125 (1994) 5–10.
[2] F.E. Bennett, E. Mendelsohn and N.S. Mendelsohn, Resolvable perfect cyclic designs, J. Combin. Theory Ser. A 29 (1980) 142–150.
[3] A.D. Keedwell, Circuit designs and Latin squares, Ars Combin. 17 (1984) 79–90.
[4] D.F. Hsu and A.D. Keedwell, Generalised complete mappings, neofields, sequenceable groups and block designs II, Pacific J. Math. 117 (1985) 291–312.
[5] C.C. Lindner and N.S. Mendelsohn, Construction of n-cyclic quasigroups and applications, Aequationes Math. 14 (1976) 111–121.
[6] N.S. Mendelsohn, Perfect cyclic designs, Discrete Math. 20 (1977) 63–68.